Mật mã & Ứng dụng

Trần Đức Khánh
Bộ môn HTTT – Viện CNTT&TT
ĐH BKHN

Chủ đề

- Hệ Mật mã không Khóa
- Hệ Mật mã khóa bí mật (đối xứng)
- Hệ Mật mã khóa công khai (bất đối xứng)
- Hàm băm, chữ ký số
- Quản lý khóa, giao thức mật mã,…

Quản lý khóa, giao thức mật mã,…

- Quản lý khóa
  - Khóa đối xứng
    - TTP
  - Khóa công khai
    - PKI

Quản lý khóa, giao thức mật mã,…

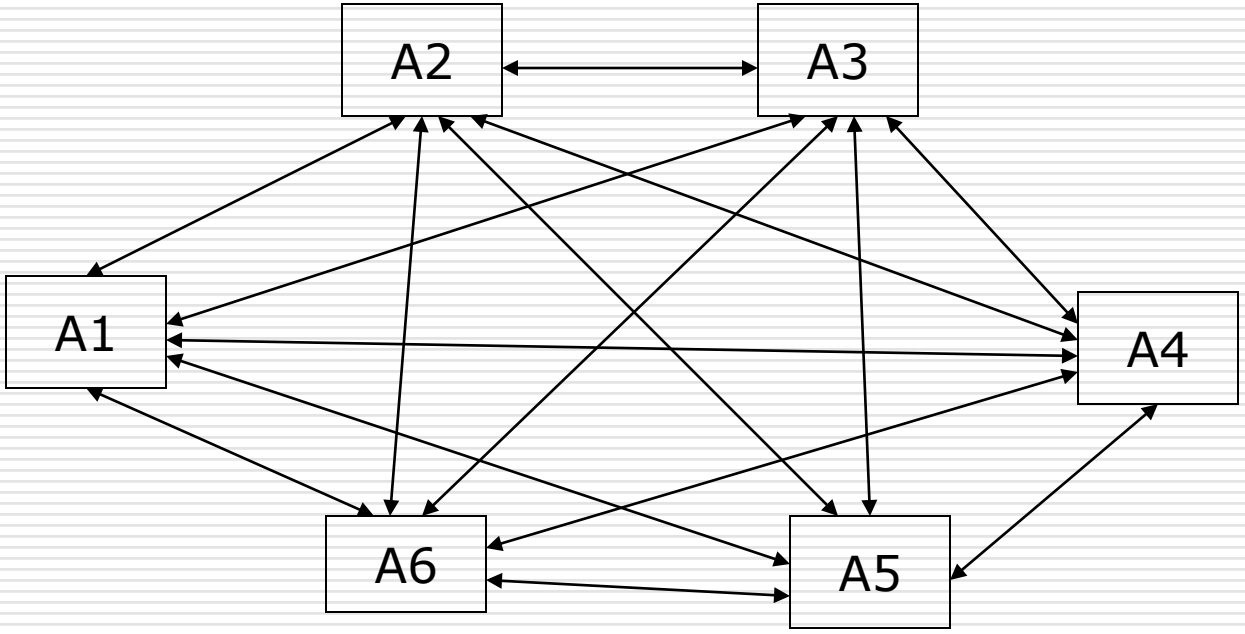
- Quản lý khóa
  - Khóa đối xứng
    - TTP
  - Khóa công khai
    - PKI

Quản lý khóa

- Quản lý khóa là một vấn đề quan trọng
  - Tính bí mật: khóa đối xứng
  - Tính toàn vẹn: khóa đối xứng, khóa công khai
- Giải pháp quản lý khóa
  - Khóa đối xứng
    - Trọng tài (Trusted Third Party)
  - Khóa công khai
    - PKI (Public Key Infrastructure)

Quản lý khóa đối xứng

- Mô hình cơ bản trao đổi thông tin khóa đối xứng



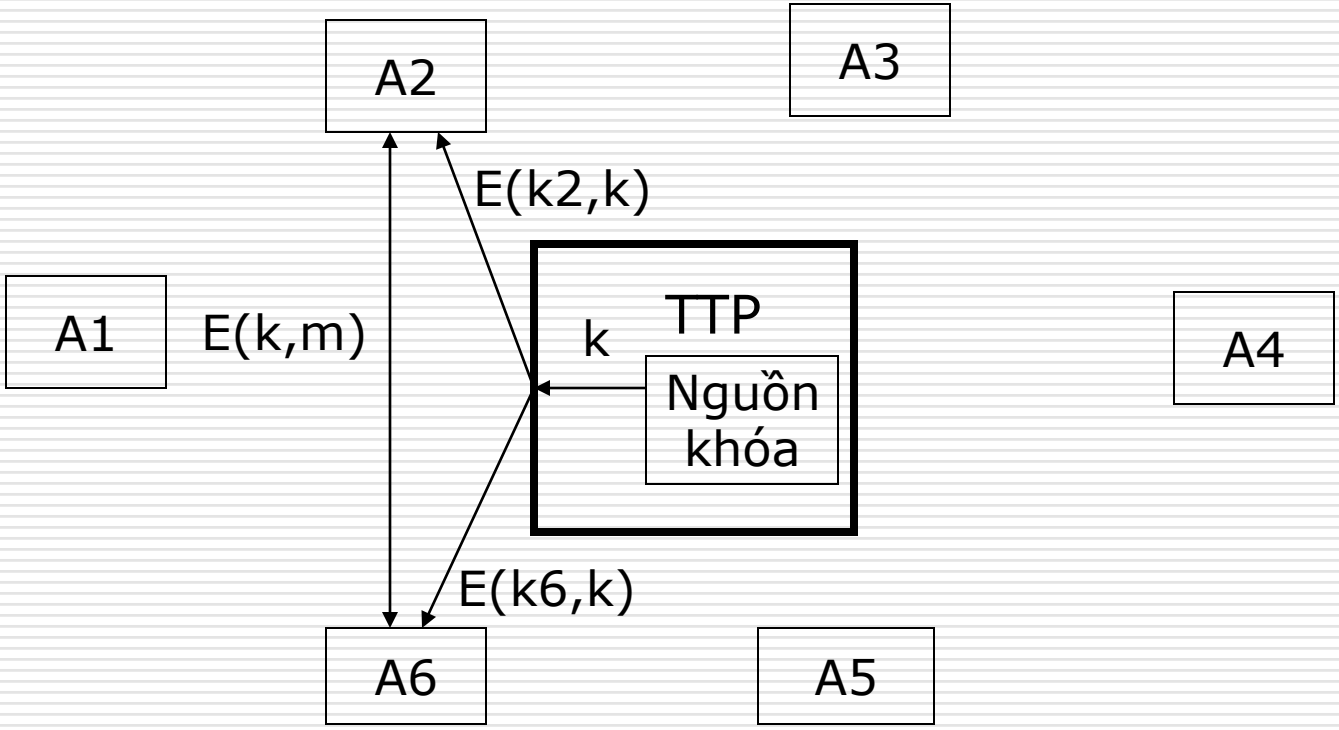
Mô hình cơ bản trao đổi thông tin khóa đối xứng

- Ưu điểm
  - Dễ dàng thêm bớt các thực thể
- Nhược điểm
  - Mỗi thực thể phải lưu trữ nhiều khóa dài hạn để trao đổi với các thực thể khác
  - Thống nhất, chia xẻ khóa khó khăn
  - Đòi hỏi các thực thể phải tin tưởng nhau

Quản lý khóa đối xứng nhờ trọng tài

- Trọng tài (Trusted Third Party)
  - Thực thể được tất cả các thực thể tham gia khác tin tưởng
  - Mỗi thực thể tham gia chia xẻ một khóa đối xứng với Trọng tài
  - Hai thực thể trao đổi thông tin bằng khóa đối xứng được Trọng tài tạo ra

Quản lý khóa đối xứng nhờ Trọng tài

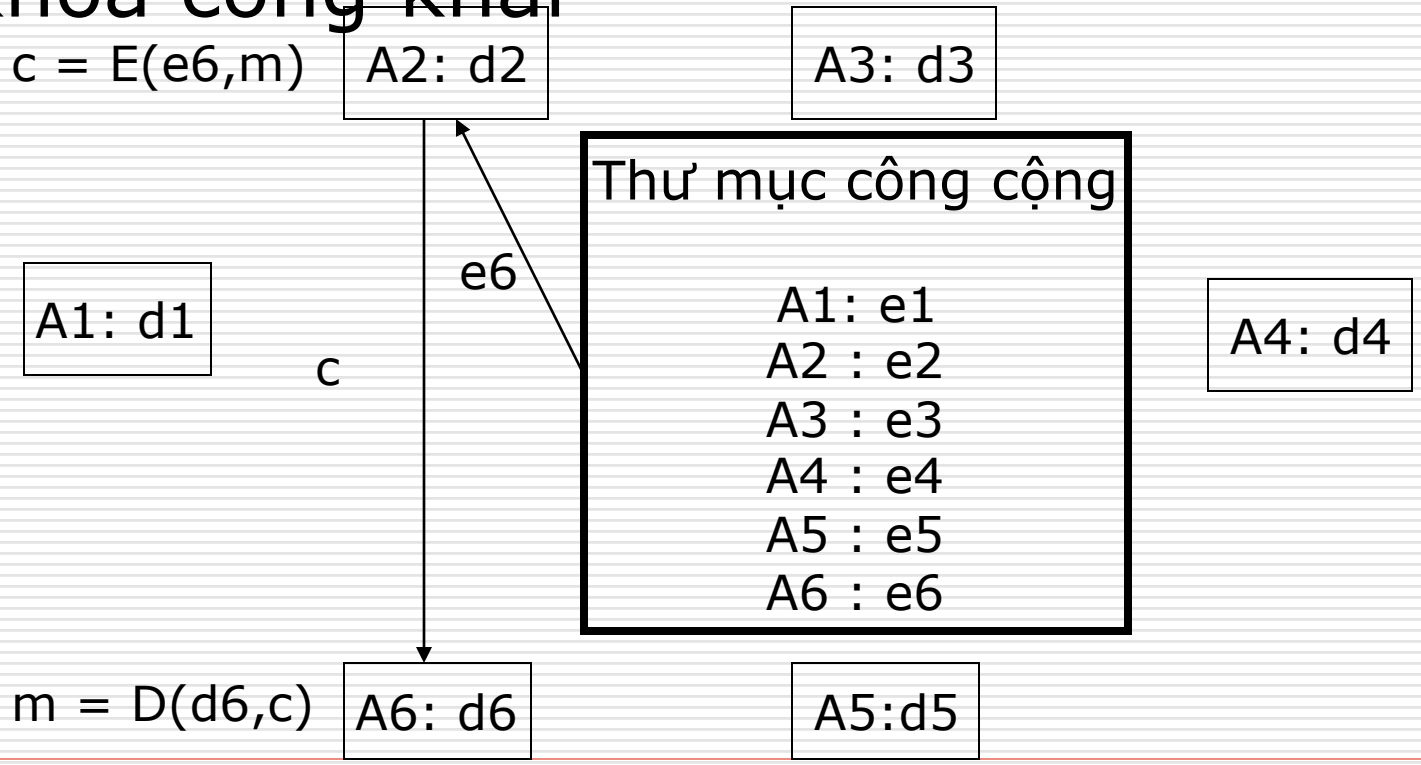


Quản lý khóa đối xứng nhờ Trọng tài

- Ưu điểm
  - Dễ dàng thêm bớt các thực thể
  - Mỗi thực thể chỉ cần lưu trữ một khóa đối xứng dài hạn
- Nhược điểm
  - Tất cả các các cuộc trao đổi thông tin đều cần tương tác ban đầu với Trọng tài
  - Trọng tài phải lưu trữ nhiều khóa đối xứng dài hạn
  - Trọng tài phải xử lý khối lượng lớn thông tin
  - Nếu Trọng tài bị đe dọa, tất cả các trao đổi thông tin đều bị đe dọa

Quản lý khóa công khai

- Mô hình cơ bản trao đổi thông tin khóa công khai

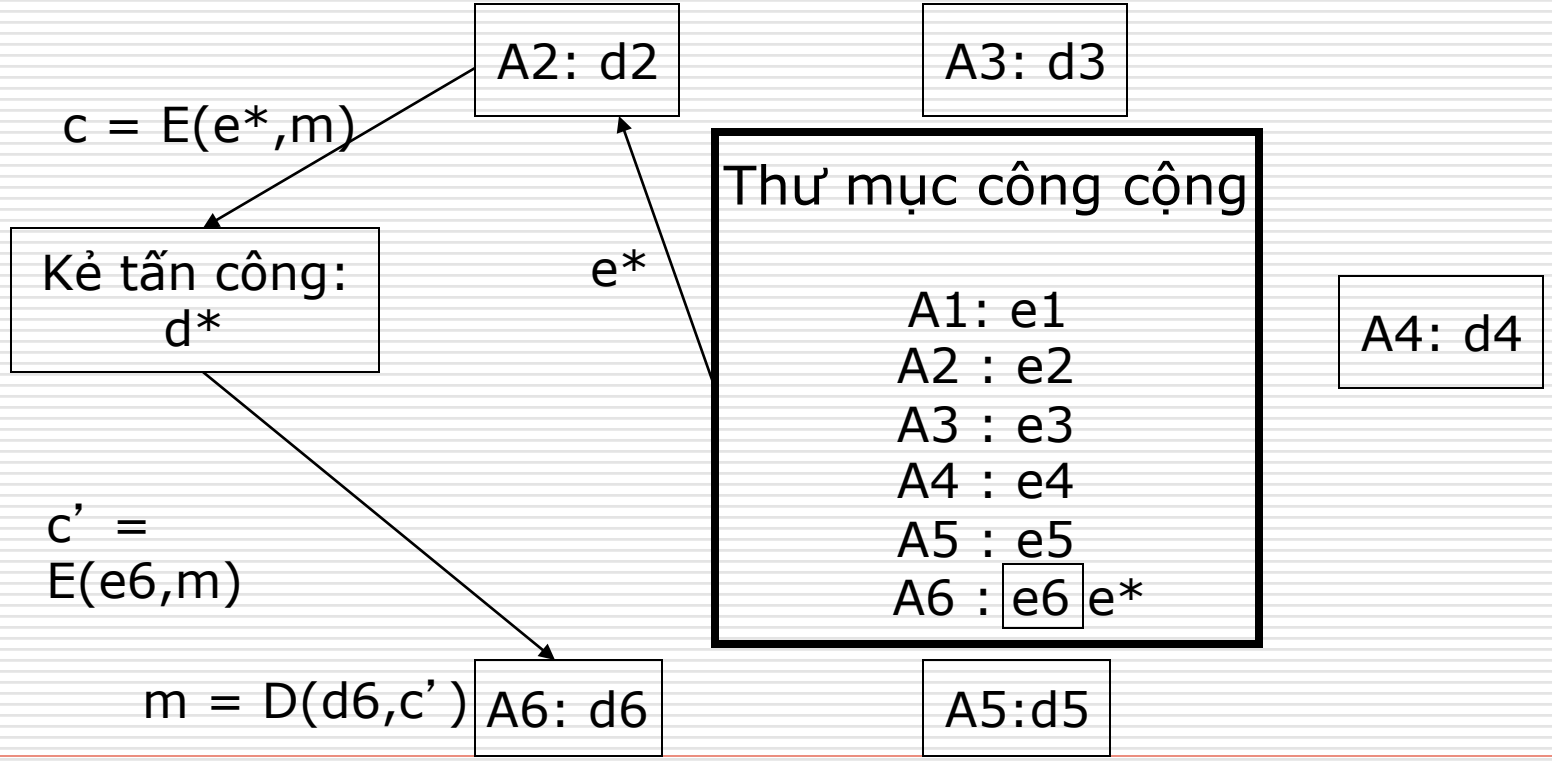


Mô hình cơ bản trao đổi thông tin khóa công khai

- Ưu điểm
  - Không cần TTP
  - Thư mục công cộng có thể được lưu trữ cục bộ cùng các thực thể
  - Số khóa lưu trữ bằng số thực thể tham gia
- Nhược điểm
  - Tấn công chủ động

Mô hình cơ bản trao đổi thông tin khóa công khai

- Tấn công chủ động



Quản lý khóa công khai nhờ PKI

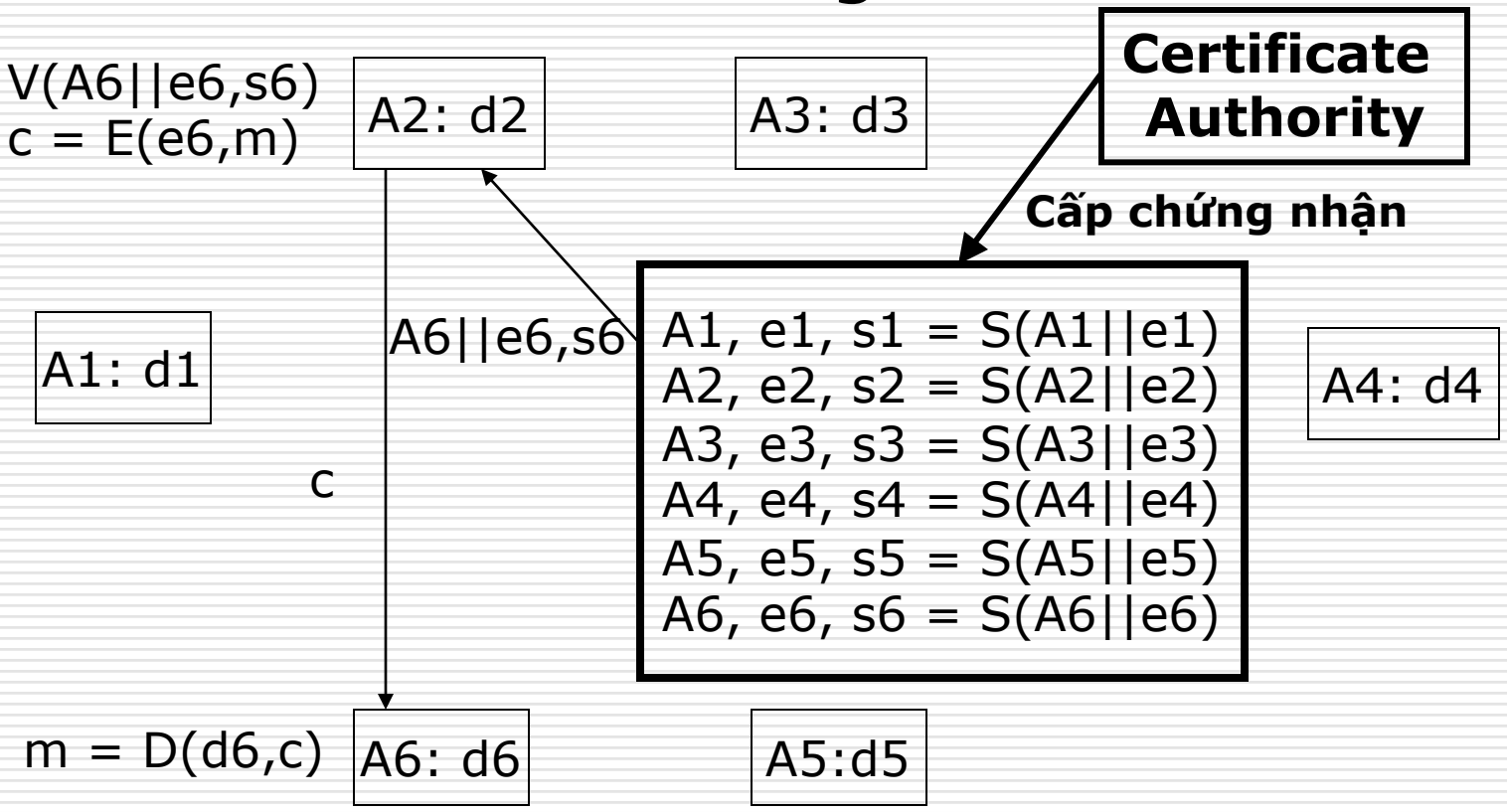
- Hạ tầng khóa công khai (PKI)
  - Là một hạ tầng an toàn trong đó các dịch vụ được xây dựng và cung cấp dựa trên các khái niệm và kỹ thuật khóa công khai
  - Mục tiêu của PKI nối khóa công khai với thực thể thông qua một thực thể được tin cậy có thẩm quyền cấp phát chứng nhận số
    - Certificate Authority

Các hợp phần của PKI

- Phát hành chứng nhận (Certificate Issuance)
  - Một hay nhiều thực thể tin cậy được quyền phát hành chứng nhận
  - Các thực thể này gọi là Certificate Authorities
- Thu hồi chứng nhận (Certificate Revocation)
  - Thu hồi chứng nhận hết hạn sử dụng
- Sao lưu/Phục hồi/Cập nhật khóa (Key Backup/ Recovery/Update)
  - Sao lưu khóa riêng
  - Phục hồi trong trường hợp bị mất
  - Cập nhật khóa để đảm bảo an toàn
- Tem thời gian (Time Stamping)
  - Thời gian cấp phát chứng nhật

Quản lý khóa công khai nhờ PKI

- Mô hình trao đổi thông tin



Quản lý khóa công khai nhờ PKI

- Ưu điểm
  - Chống tấn công chủ động
  - CA chỉ cấp chứng nhận, không tham gia vào việc trao đổi thông tin giữa các bên
  - Có thể giảm thiểu tương tác với CA bằng cách lưu các chứng nhận cục bộ
- Nhược điểm
  - Nếu thuật toán sinh chữ ký của CA bị đe dọa, tất cả các trao đổi thông tin đều bị đe dọa
  - Độ tin cậy hoàn toàn dựa trên CA